Eléments Mathématiques sur les Groupes et un peu de théorie des Nombres.

En préparation pour le passage de l'algo de Simon vers l'algo de Shor pour la fact des entiers naturels.

#1.

1) Groupes Abéliens et les classes d'équivalence

Groupe fini $G = \{g_1, g_2, \dots, g_N\}$

opération de groupe noté multiplicativement

$g_1 \in G$ et $g_2 \in G$ alors $\boxed{g_1 g_2 \in G}$.

(notation additive $g_1 + g_2 \in G$).

1) Associativité $(gg')g'' = g(g'g'')$

2) $\exists\, e \in G$ t.q $ge = eg = g$ (élément neutre)

3) $\exists$ inverse pour tout g : $g^{-1}g = gg^{-1} = e$

On dira que le groupe est commutatif si

$$g g' = g' g \quad .$$

Ici on va s'occuper uniquement de G commutatifs

Notion de sous-groupe. $H \subset G$ t.q

- si h et $h' \in H$ alors $hh' = h'h \in H$
- si $h \in H$ alors $h^{-1} \in H$.

en conséquence $h h^{-1} = h^{-1} h = e \in H$.

de plus l'associativité est aussi vérifiée dans H puisqu'elle est vraie dans G et que la loi est stable de H.

$\Rightarrow$ un sous-groupe $H \subset G$ est aussi un groupe

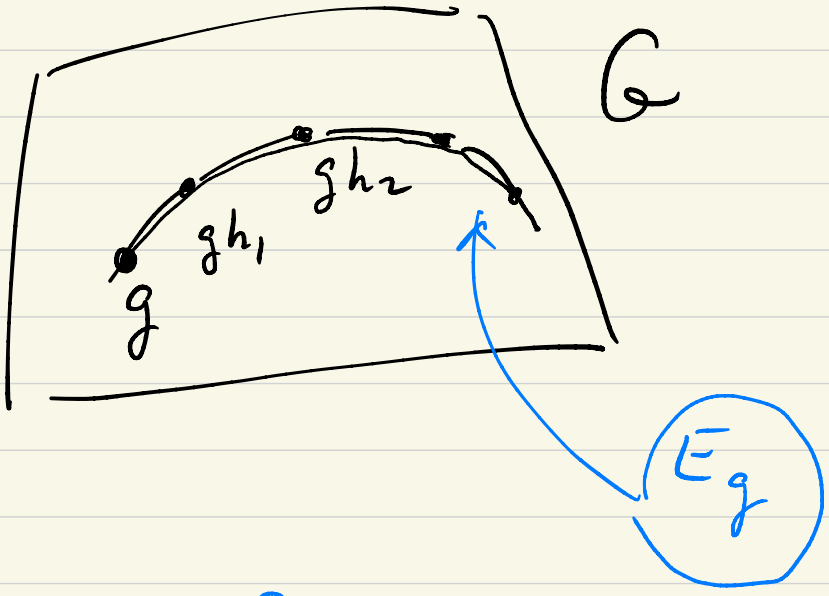
Remarque $H = \{e\}$ et $H = G$ sont deux sous groupes triviaux qui existent toujours.

Classe d'équivalence d'un sous groupe HCG.

Def : pour chaque élément $g \in G$ la classe d'équivalence associée

$$E_g = \{ gh \mid h \in H \}.$$

il s'agit de l'ensemble atteignable à partir de g en agissant avec tous les éléments de H



Quand G est commutatif on peut agir à gauche ou à droite

$$E_g = \{ gh \mid h \in H \} = \{ hg \mid h \in H \}.$$

Propriété fondamentale : Si $g \neq g'$ dans G

alors { ou bien $E_g = E_{g'}$
ou bien $E_g \cap E_{g'} = \emptyset$.

Théorème de Lagrange :

(i) Soit g et $g' \in G$. Alors on a deux possibilités : $E_g = E_{g'}$ ou $E_g \cap E_{g'} = \emptyset$

(ii) Le nombre de classes d'équivalences est égal à $\frac{|G|}{|H|} = \frac{\text{Card}(G)}{\text{Card}(H)}$ et en particulier $|H|$ doit nécessairement diviser $|G|$.

Notation : L'ensemble des classes d'équiv est noté G/H (ensemble) et sa cardinalité $|G/H| = \frac{|G|}{|H|}$ (nombre entier).

Preuve du point i)

Fixons g et $g' \in G$. Si $E_g \cap E_{g'} = \emptyset$ alors rien à prouver. Sinon $E_g \cap E_{g'} \neq \emptyset$ et $\exists\ \bar{g} \in E_g \cap E_{g'}$. Du coup puisque

$\bar{g}$ et g sont dans E_g, $\exists\ h \in H$ t.q

$$\bar{g} = gh. \quad (*)$$

aussi puisque $\bar{g}$ et g' sont dans $E_{g'}$, $\exists\ h' \in H$

t.q $\bar{g} = g'h'$ $(*)$

$$(*) \Rightarrow gh = g'h' \Rightarrow g \underbrace{hh'^{-1}}_{\in H} = g'$$

$$\Rightarrow \boxed{g' \in E_g} = (a)$$

Mais encore $g'h'h^{-1} = g \Rightarrow \boxed{g \in E_{g'}} = (b)$

(a) $E_{g'} \subset E_g$
(b) $E_g \subset E_{g'}$
$\Rightarrow \boxed{E_g = E_{g'}}$. ∎

Preuve de (ii) :

On remarque simplement que

$$|E_g| = |\{gh \mid h \in H\}| = |H|.$$

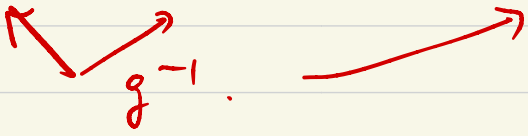
En effet l'application :

$$H \longrightarrow E_g$$

$$h \longmapsto gh = f(h)$$

est une bijection.

- injection car $gh_1 = gh_2 \Rightarrow h_1 = h_2$



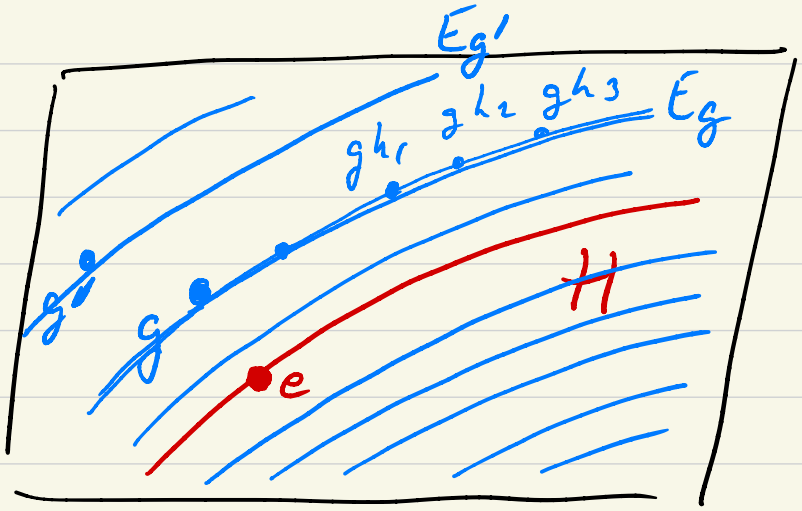
- surjection $(gh)\, g^{-1} = h$.

Par conséquence $|G/H| \cdot |H| = |G|$.

$$\Rightarrow \underbrace{|G/H|}_{\text{entier}} = \frac{|G|}{|H|}.$$

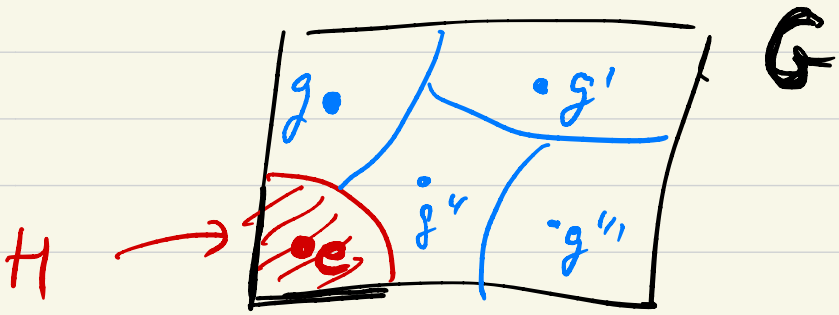
et nécessairement $|H|$ doit diviser $|G|$.

Image qui suit le Thm de Lagrange.



H ⊂ G sous groupe

- sous-groupe H est la classe d'équ de l'élément neutre e.
- les classes d'équivalences sont toutes distinctes et forment un feuilletage de G ou si vous voulez une partition de G.
- Autre image possible :



Exemples simples.

loi de groupe : addition mod 2

① $G = \left(\mathbb{F}_2^n, \oplus\right)$ esp vect des vect binaires à n composante.

$$H = \{ \underline{0}, \underline{a} \} \quad 0 \neq \underline{a} \in \mathbb{F}_2^n$$

$$|G| = 2^n, \quad |H| = 2, \quad |G/H| = \frac{|G|}{|H|} = 2^{n-1}$$

$$E_{\underline{x}} = \{ \underline{y} = \underline{x} \oplus \underline{a} \}.$$

exercice $n = 3$ et $\underline{a} = (0, 1, 0)$

dessin des classes d'équiv dans le cube de Hamming.

Aussi à faire pour $\underline{a} = (0, 1, 1)$ et $\underline{a} = (1, 1, 1)$

② $G = \left(\mathbb{F}_2^n, \oplus\right)$ et $H =$ sous-esp vect de dimension k.

$$|G/H| = \frac{|G|}{|H|} = 2^{n-k}.$$

$$|H| = 2^k$$

$$\underline{h} = \alpha_1 \underline{h}_1 \oplus \alpha_2 \underline{h}_2 \oplus \cdots \oplus \alpha_k \underline{h}_k$$

$\alpha_i \in \{0, 1\}$

③ $G = (\mathbb{Z}, +)$ entiers naturels munis de l'addition usuelle.

$H = r.\mathbb{Z}$ avec r entier positif.

ensemble des multiples de r.

$\{\dots, -2r, -r, 0, r, 2r, 3r, 4r, \dots\} = H$.

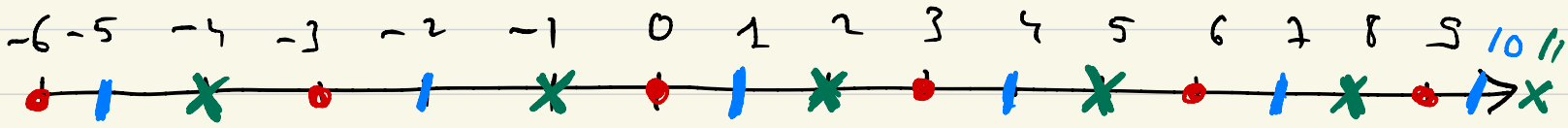
↗

Sous-groupe de $\mathbb{Z}$.

Classes d'équivalence ici ?

$0 \rightarrow H = r\mathbb{Z} . \dots, 0+r, 0+2r, \dots$

$q \rightarrow q + m.r$ $r = 3$ $q = 1$



$\mathbb{Z}$

$r=3$: 3 classes d'équiv E_0, E_1, E_2. ||

ici ne sont rien d'autre que les entiers pris G

modulo 3.

$= \frac{\mathbb{Z}}{3\mathbb{Z}} = \frac{G}{H}$.

En général les classes d'équiv $\frac{\mathbb{Z}}{r\mathbb{Z}}$ entiers mod r.

$$\left| \frac{\mathbb{Z}}{r\mathbb{Z}} \right| = r .$$

Les entiers mod r $= \{0, 1, 2, \dots, r-1\}$.

$=$ l'ensemble $\frac{\mathbb{Z}}{r\mathbb{Z}}$ des classes d'équivalence des sous-groupes $r\mathbb{Z}$ du groupe $\mathbb{Z}$.

(4) $G = \left(\frac{\mathbb{Z}}{M\mathbb{Z}}, +\right) = \{0, 1, 2, \dots, M-1\}$.

entiers mod M c.-à-d que $+$ est faite modulo M.

avec M entier (grand).

$H = \underbrace{r\mathbb{Z}}_{\text{multiples de } r}$ inclus dans $\{0, 1, 2, \dots, M-1\}$.

- Quand est-ce que H est un sous groupe de G ?

Nécessairement il faut que r divise M. à cause du Thm de Lagrange → Réfléchir à ceci.

Si r ne divise pas M alors H n'est pas s-groupe de G.